

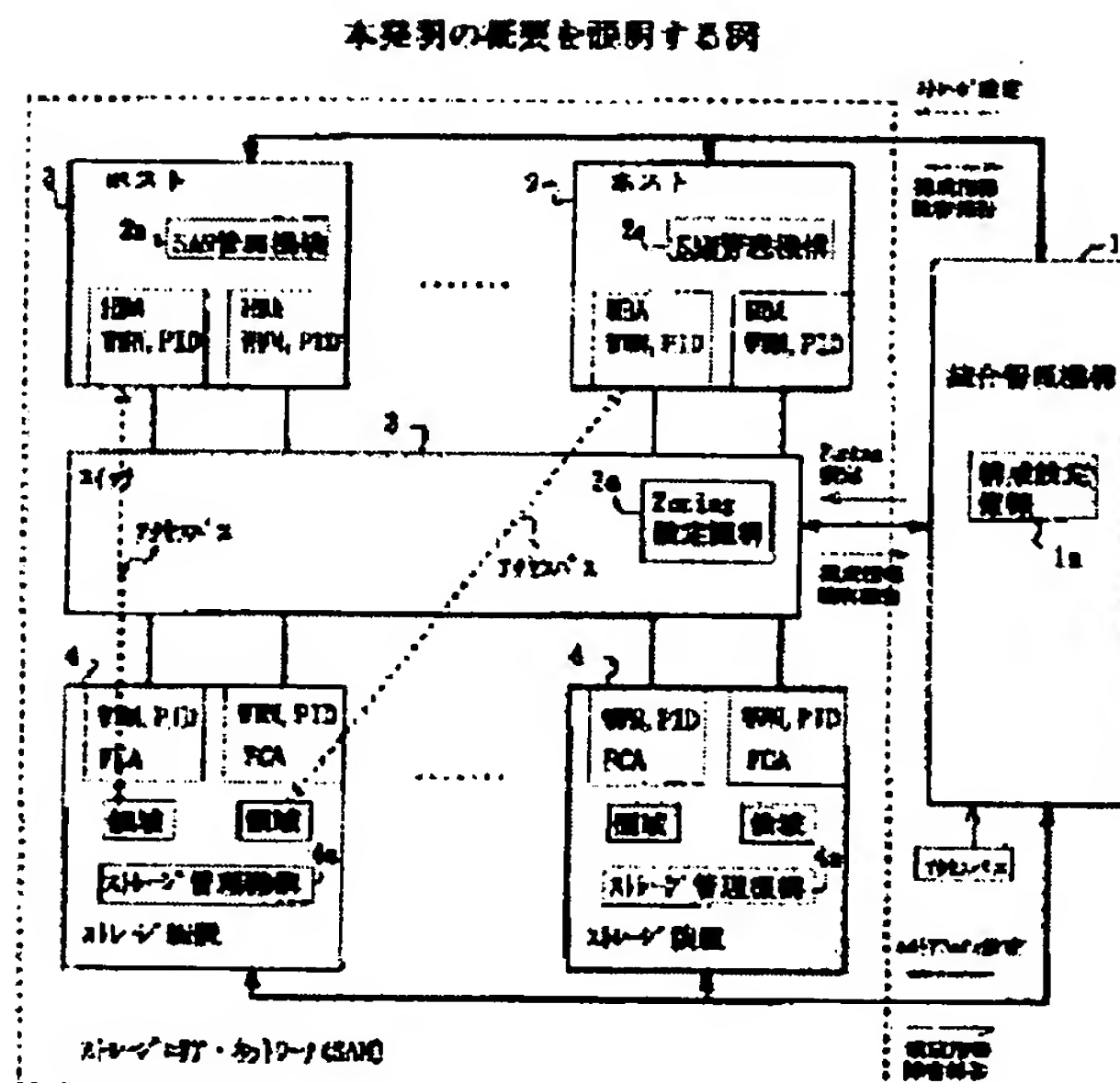
STORAGE AREA NETWORK MANAGING SYSTEM

Patent number: JP2002063063
 Publication date: 2002-02-28
 Inventor: IWATANI SAWAO
 Applicant: FUJITSU LTD
 Classification:
 - international: G06F12/00; G06F12/14
 - european:
 Application number: JP20010167946 20010604
 Priority number(s): JP20010167946 20010604; JP20000167482 20000605

Report a data error here

Abstract of JP2002063063

PROBLEM TO BE SOLVED: To automatically perform best security management for a SAN (storage area network) by unitarily integrating/managing conventional discrete security methods. **SOLUTION:** An integrating/managing mechanism 1 for integrating/managing SAN is installed, so that access relations between hosts 2 and storage devices 4 can be collectively managed by using the managing mechanism 1. Access paths, that is, areas on the storage device 4 side which are to be accessed from the host 2 side, and fiber channel adaptors(FCAs) and host bus adaptors(HBAs), which are used when the storages are accessed, are set in the mechanism 1. Based on access path information set, the mechanism 1 performs storage settings, a zoning setting, and settings for which area to permit access, for SAN managing mechanism 2a of the hosts 2, a zoning setting mechanism 3a of a switch 3, and storage managing mechanisms 4a of the storage devices 4, respectively.



Data supplied from the esp@cenet database - Worldwide

(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-63063

(P2002-63063A)

(43)公開日 平成14年2月28日(2002.2.28)

(51)Int.Cl. ⁷	識別記号	F I	テ-マコ-ト ⁷ (参考)
G 0 6 F 12/00	5 4 5	G 0 6 F 12/00	5 4 5 B 5 B 0 1 7
	5 3 7		5 3 7 A 5 B 0 8 2
12/14	3 2 0	12/14	3 2 0 A

審査請求 未請求 請求項の数9 O L (全 20 頁)

(21)出願番号 特願2001-167946(P2001-167946)
(22)出願日 平成13年6月4日(2001.6.4)
(31)優先権主張番号 特願2000-167482(P2000-167482)
(32)優先日 平成12年6月5日(2000.6.5)
(33)優先権主張国 日本(J P)

(71)出願人 000005223
富士通株式会社
神奈川県川崎市中原区上小田中4丁目1番1号
(72)発明者 岩谷 沢男
神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内
(74)代理人 100100930
弁理士 長澤 俊一郎 (外1名)
Fターム(参考) 5B017 AA03 BA06 CA07
5B082 EA11

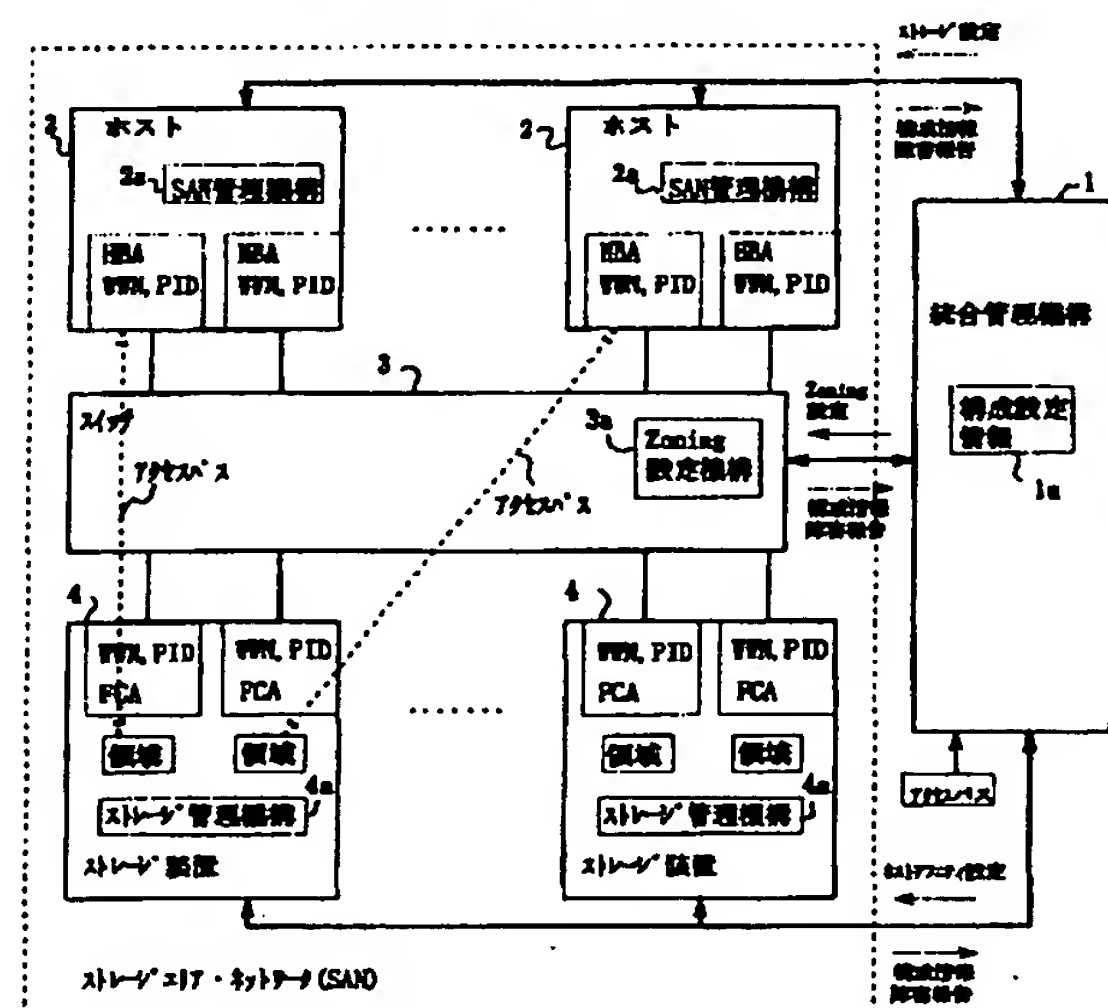
(54)【発明の名称】 ストレージエリア・ネットワーク管理システム

(57)【要約】

【課題】 従来の分割されたセキュリティ方式を一元的に統合管理し、SANにおいて最善のセキュリティ管理を自動的に行うこと。

【解決手段】 SANを統合制御する統合管理機構1を設置し、ホスト2とストレージ装置4とのアクセス関係をこの管理機構1を用いて一括して管理できるようにする。統合管理機構1にアクセスパス、すなわち、ホスト2側からアクセスをしようとするストレージ装置4側の領域と、そのストレージをアクセスする際の使用するファイバチャネルアダプタ(FCA)、ホストバスアダプタ(HBA)を設定する。設定されたアクセスパス情報を元に、統合管理機構1は、ホスト2のSAN管理機構2a、スイッチ3のゾーニング(Zoning)設定機構3a、ストレージ装置4のストレージ管理機構4aに、それぞれストージ設定、ゾーニング設定、アクセスをどこの領域に対して許可するかの設定を行う。

本発明の概要を説明する図



ンピュータについてのアクセス制限情報を通知し、ホストとストレージとのアクセス関係を一括して管理することを特徴とするストレージエリア・ネットワーク・システムを統合制御するプログラムを記録した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はファイバチャネル・ネットワークを用いて複数のサーバ／複数のストレージを結合するストレージエリア・ネットワーク（以下SANと呼ぶ）の管理システムに関する。

【0002】

【従来の技術】近年、1台のストレージ・システムの容量が大きくなり、複数の多種多様なサーバから使用できるような機能が求められている。また、データ転送経路に高速かつ複数ホスト・ストレージ間の並列転送が可能なファイバチャネルが普及し始めたことをきっかけに、この環境での接続形態はさらに大規模化すると考えられている。このような複数のサーバ／複数のストレージ結合をストレージエリア・ネットワーク（以下SANという）と呼び、分散化されつつある複数サーバのストレージの一元的管理やTOCの削減を計ろうとする試みが進みつつある。

【0003】

【発明が解決しようとする課題】しかしながら、ストレージ内の領域管理や、セキュリティの面で解決しなければならない問題がある。その一つに、SANが複数のホストコンピュータ（以下ホストという）及び複数のストレージ・システムより構成されていた場合に、全てのホストから全てのストレージ・システムがアクセス可能である為に、あるホストから使用しているストレージ内のデータが他のホストから不用意に破壊されてしまう可能性があった。

【0004】ストレージ内の領域管理や、セキュリティの面で完全な対策となるものがないのが現状である。また、SANを構成する複数装置で障害が発生した際、いろいろなエラー報告がシステム管理者に報告される為、被疑箇所を特定することが難しく方法がなかった。本発明は上記事情を考慮してなされたものであって、本発明の目的は、従来の分割されたセキュリティ方式を一元的に統合管理し、SANにおいて最善のセキュリティ管理を自動的に行うことができるようにすることである。

【0005】

【課題を解決するための手段】図1は本発明の概要を説明する図である。同図に示すように、本発明は上記SAN環境に対して、SANを統合制御する統合管理機構1を設置し、ホスト2とストレージ装置4とのアクセス関係をこの管理機構1を用いて一括して管理できるようにする。システム管理者は、統合管理機構1にホスト2側からアクセスをしようとするストレージ装置4側の領域と、そのストレージをアクセスする際の使用するファイ

バチャネル・アダプタ（FCA）、ホストバス・アダプタ（HBA）を設定する。この設定をアクセスパスと呼ぶ。設定されたアクセスパス情報を元に、この統合管理機構1は、まずホスト2側から見えるストレージ設定

（Storage affinity）をホスト2側のSAN管理機構2aに設定する。また、スイッチ3のゾーニング（Zoning）設定機構3aに対して、FCA、HBAが保有するWWN、PID情報を事前に確保しておきこれを元に設定されたアクセスパスが実現できるように計算してゾーニング（Zoning）を設定する。さらに、ストレージ装置4のストレージ管理機構4aには、ストレージ装置のどのFCAがどこのHBA（WWN、PID）のアクセスをどこの領域に対して許可するかの設定を行う。上記のような統合管理機構1を設けることにより、SANにおいて、セキュリティ管理やストレージ内の領域管理を一括して行うことができる。また、上記統合管理機構に、SANの構成状態を構成設定情報1aとして保持させることにより、SANに、SAN管理機能を持たないホストや、ゾーニング設定機能を持たないスイッチや、あるいはストレージ管理機能を持たないストレージ装置が投入されても容易に対応することができ、可能な範囲でセキュリティを確保することができる。

【0006】さらに、上記統合管理機構1を設けることにより、以下の機能を実現することができる。

（1）統合管理機構1が、SANの構成状態を個々の装置より確保して、構成設定情報1aとして格納し、定期的もしくは、システム管理者からのコマンド指示によって、統合管理機構1が、現状のSANの構成状態を読み込み、SANの構成設定情報1aと比較し、異なっていた場合は、異常と判断し、システム管理者に通知する。これにより、システム管理者はSANの異常を容易に知ることができる。

（2）統合管理機構1が、システム管理者からのコマンド指示によって、SAN管理機構2a、Zoning設定機構3a、ストレージ管理機構4aよりアクセス関係情報を確保してアクセスパスの整合性を確認する。アクセスパスが正しく設定されていない場合は、その部分を異常とシステム管理者に通知する。これにより、システム管理者はアクセスパスの整合性を確認することができる。

（3）ホスト2、ホスト2のHBA、スイッチ3、あるいは、ストレージ装置3のFCAが交換されたとき、上記統合管理機構1はこれを検知し、ホスト2のSAN管理機構2a、スイッチ3のゾーニング設定機構3a、もしくは、ストレージ装置4のストレージ管理機構4aから、交換後の設定情報を取得し、交換前と同等のアクセス関係を構築するように再度アクセス関係を設定する。これにより、SANの構成変更に対して容易に対処することができる。

（4）システム起動時にアクセスパスが設定されてい

0, 420にはストレージ管理機構418, 428を設置する。

【0011】SAN管理機構とは前記a)で説明したストレージ・アフィニティの設定を行える機構であり、ストレージ管理機構は前記したc)で説明したホスト・アフィニティの設定が行える機構である。さらに、スイッチ300には前記b)で説明したスイッチのゾーニング設定機構301が搭載される。システム管理者は、SAN統合管理機構500にホスト側からアクセスをしようとするストレージ側の領域と、そのストレージをアクセスする際の使用するFCA（ファイバチャネル・アダプタ）、HBA（ホストバス・アダプタ）を設定する。この設定をアクセスパスの設定と呼ぶ。設定されたアクセスパス情報は、このSAN統合管理機構500の中で、図5（a）に示すSAN統合管理機構500内アクセスパス設定情報の様に格納される。この設定情報を元に、まずホスト側から見えるストレージ設定（Storage affinity）をホスト側のSAN管理機構118, 128に設定する。すなわち、どのHBAからどのFCA（WWN, PID）へのアクセスを行うかを設定する。

【0012】また、どのHBAからどのFCAに対してアクセスするかの設定は、図5（b）に示すストレージ・アフィニティ（Storage Affinity）テーブルのような管理テーブルをホスト内で作成し、アクセスするFCAを選択させる事で実現する。この例では、HBA111からWWNcのFCAに対して領域415をアクセスするように設定している。ファイバチャネル上のコマンドは、相手FCAのWWNを介して発行する事が出来る。さらに、スイッチ300のゾーニング（Zoning）設定機構301に対して、FCA, HBAが保有するWWN, PID情報を事前に確保しておき、これを元に設定されたアクセスパスが実現できるように計算してゾーニング（Zoning）を設定する。図5（c）にスイッチ・ゾーニング（Zoning）テーブルの例を示す。ここではゾーン（Zone）をAとBで設定し、それぞれのゾーン（Zone）に相互アクセスを許可するポート（HBA, FCA）の識別子（ここではWWN）を格納する。これにより、スイッチWWNaからアクセスはゾーン（Zone）Aと認識し、WWNcに対してのみしか実行できないようなアクセス制限を行う。

【0013】ファイバチャネル環境ではスイッチ300とポートを接続するとログインシーケンスが動作し、その中でスイッチはポートのWWN情報を確保できる。この情報を元に、ホスト110, 120からストレージ装置410, 420にコマンドが発行された場合に、ゾーン（Zone）設定されていないポートに対するアクセスが指定された時、ストレージ装置410, 420のポートにコマンドが伝わらないような制御を行う。さらに、ストレージ装置410, 420のストレージ管理機構418, 428には、ストレージ装置410, 420のどの

HBA, PIDからのアクセスを、何処の領域に対して許可するかの設定を行う。図5（d）にホスト・アフィニティ（Host affinity）テーブルの例を示す。このテーブルにより、FCA411はWWNaのHBAからのアクセスのみを領域415に対して許可し、FCA412はWWNeのHBAからのアクセスのみを領域416に対して許可する。

【0014】ファイバチャネル環境ではホストからのコマンドを受け付ける前に、ログインシーケンスという相互のポートの情報をやりとりするシーケンスがあり、その中で相手のWWNやPIDなどを確認できる。FCAは、ここで確保した相手のWWNやPIDの情報がアクセス許可されているものかどうかを判断し、アクセス許可がされたものに対してのみ処理を継続し、アクセス許可されていないものからのアクセスに対しては、チェックコンディション（Check condition）等でエラー応答を行う。なお、SANを構成するホスト装置のなかにはSAN管理機構をもたない装置がある。また、ストレージ装置内でも前記c)のホスト・アフィニティ機能を提供していない装置もある。したがって、そのような装置に対して管理機構500はアクセス関係を設定しないが、他のセキュリティ方式（Storage Affinity もしくはZoning）によってセキュリティは保護される。

【0015】図6によりSAN統合管理機構500が行う作業のフローチャートとその作業の具体例を説明する。まず、SAN統合管理機構500は、各FCA, HBAのWWN及びPIDを読み込む（ステップS1）。図3の例においては、SAN統合管理機構500が例えばホスト110のHBA111がWWNa, PIDaであり、ストレージ装置410のFCA411がWWNc, PIDc、FCA412がWWNd, PIDd等であることを認識する。ついで、SAN統合管理機構500は、HBAからアクセスする予定のFCAと、その配下の領域を受け付ける（ステップS2）。図3の例においては、例えばホスト110のHBA111からストレージ装置410のFCA411経由で領域415にアクセスするパス設定を受け付ける。

【0016】次に、当該ホストがストレージ・アフィニティ（Storage Affinity）機能をサポートしているかを調べる（ステップS3）。ストレージ・アフィニティ（Storage Affinity）機能をサポートしていない場合にはステップS5に行く。また、ストレージ・アフィニティ（Storage Affinity）機能をサポートしている場合にはステップS4において、ストレージ・アフィニティ（Storage Affinity）機能により、SAN統合管理機構500は、ホスト側のSAN管理機構に、HBAからアクセスできるデバイスをWWNもしくはPIDを使用して設定する。例えば図3の例においては、ホスト110のHBA111から、ストレージ装置410のFCA411の識別子であるWWNcもしくはPIDcをアクセスできるよう

ANの構成設定情報501と比較して、異なっていた場合は、異常と判断してシステム管理者に通知する。例えば、前記図3の状態時にSANの構成設定情報501を登録し、その後ストレージ420の電源が落ちてしまった場合は、SANの構成状態異常と判断して、システム管理者にストレージ420が見えなくなっていることを通知する。

【0024】(2) アクセスパスの整合性の確認

SAN統合管理機構500は、システム管理者からのコマンド指示によって、SAN管理機構118、128、ゾーニング (Zoning) 設定機構301、ストレージ管理機構418、428よりアクセス関係情報を確保してアクセスパスの整合性を確認する。アクセスパスが正しく設定されていない場合は、その部分を異常とシステム管理者に通知する。この機能によりシステム管理者が勝手に個々の機器の設定を変えてしまった場合に、異常点を検出することが可能となる。また、既に、SANがアクセスパスの設定がされた状態で存在し、新たに当該SAN管理論理を組み込む際に、既存のSANのアクセスパスが正しく設定されているかチェックすることができる。

【0025】(3) HBAの交換時のアクセス関係の再設定

ホスト110側のHBA111が故障して新たなHBAに交換された場合、SAN管理機構118はHBA交換を検知して、システム管理者に通知する。システム管理者からの構成再設定コマンドによって、SAN管理機構118はSAN統合管理機構500に交換された新しいHBAのWWNを伝える。SAN統合管理機構500はその新しいWWNを用いてHBA交換前と同等のアクセス関係を構築し、二つのアクセス関係を設定する機構〔ゾーニング (Zoning) 設定機構301、ストレージ管理機構418〕に再度アクセス関係を設定する。

【0026】(4) ホスト交換時のアクセス関係の再設定

ホスト110が故障して新たなホストに交換された場合に、ホスト110のSAN管理機構118は設定がなくなっている事検知して、システム管理者に通知する。システム管理者からの構成再設定コマンドによって、SAN管理機構118はSAN統合管理機構500に接続されているHBAのWWNを伝え、SAN統合管理機構500は、そのWWNを用いてHBA交換前と同等のアクセス関係を構築し、二つのアクセス関係を設定する機構〔ゾーニング (Zoning) 設定機構301、ストレージ管理機構418〕に再度アクセス関係を設定する。

【0027】(5) スイッチ交換時のアクセス関係の再設定

スイッチ300が故障して交換された際に、スイッチに設定したゾーニング (Zoning) 情報がなくなっている事検出し、システム管理者に通知する。SAN統合管理

機構500に、システム管理者からの構成再設定コマンドによって、新しいスイッチに故障前のアクセス関係をセットさせる機構を設け、このような場合に、SAN統合管理機構500から、新しいスイッチに故障前のアクセス関係を再設定する。なお、スイッチ300が故障して交換された際に、スイッチに設定したゾーニング (Zoning) 情報がなくなっている事検出するが、システム管理者には通知せず、自動的にSAN統合管理機構500から新しいスイッチに故障前のアクセス関係をセットさせる機構をSAN統合管理機構500に設け、再設定できるようにしてもよい。

【0028】(6) FCA交換時のアクセス関係の再設定

ストレージ装置側410のFCA411が故障し交換され、FCA側のWWNが変更されてしまった場合に、これを検出しシステム管理者に通知する。システム管理者からの構成再設定コマンドによって、ストレージ管理機構418が新しいFCAのWWNを検出してSAN統合管理機構500に伝え、SAN統合管理機構500はその新しいWWNを用いてFCA交換前と同等のアクセス関係を構築し、二つのアクセス関係を設定する機構〔SAN管理機構118、ゾーニング (Zoning) 設定機構301〕に再度アクセス関係を設定する。

【0029】(7) 不用意なアクセスの設定の防止

前述したように、システム起動時にアクセスパスを設定していない状態で、不用意なアクセスが設定されることを防ぐ為に、システム起動時にアクセスパスが設定されていない状態時に、スイッチに対して全てのアクセスを許可しない設定を行う。このような設定がないと、全てのSANのストレージに対して全てのホストからアクセス出来てしまい、セキュリティ上の問題が生ずることがある。

(8) ファイバチャネルの転送クラスの設定

ファイバチャネル (FC) ではHBAとFCA側で共通に設定すべきFCの転送クラス (Class) というパラメータがある。転送クラスにはクラス1~3があり、転送クラス1は殆ど使用されず、転送クラス2は転送後、アクノリッジを返し、転送クラス3は転送後、アクノリッジを返さない転送方式である。このパラメータがHBA側とFCA側で異なっていると転送ができない。そこで、前記したアクセスパスを設定する際に、使用するClassもシステム管理者に指定させて、管理機構500がSAN管理機構118、128、ストレージ管理機構418、428を通じて、アクセスパスを設定したHBAとFCAが指定された同一のClassで動作させるようにする。

【0030】次に、上記SAN統合管理機構500を用いたSANの障害監視について説明する。基本的にSAN統合管理機構500を用いた場合は、SANを構成する装置 (ホスト、スイッチ、ストレージ装置) で発生し

もに、該アクセス経路情報に基づき、ホストコンピュータのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知し、スイッチの領域設定機構に対して領域情報を通知し、ストレージ装置のストレージ管理機構に対して上記ホストコンピュータについてのアクセス制限情報を通知することを特徴とするストレージエリア・ネットワーク管理システム。

(付記2) 上記統合管理機構は、ストレージエリア・ネットワークの構成状態を個々の装置より取得して、ストレージエリア・ネットワークの構成設定情報として保持し、定期的もしくは、システム管理者からの指示によって、現状のストレージエリア・ネットワークの構成状態を集収し、上記構成設定情報と集収した現状の構成情報とを比較することにより、ストレージエリア・ネットワーク・システムの異常を判断することを特徴とする付記1のストレージエリア・ネットワーク管理システム。

(付記3) 上記統合管理機構は、ホストコンピュータのストレージエリア・ネットワーク管理機構、スイッチ、および/またはストレージ装置より、アクセス関係情報を取得して、アクセスパスの整合性を確認し、アクセスパスが正しく設定されていないとき、その部分を異常として通知することを特徴とする付記1または付記2のストレージエリア・ネットワーク管理システム。

(付記4) 複数のホストコンピュータと複数のストレージ装置が、スイッチを介して接続されたストレージエリア・ネットワーク・システムであって、上記ストレージエリア・ネットワークを統合制御する統合管理機構を備え、該統合管理機構はホストコンピュータとストレージ装置とのアクセス経路情報を備えるとともに、該アクセス経路情報に基づき、ホストコンピュータのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知し、スイッチの領域設定機構に対して領域情報を通知し、ストレージ装置のストレージ管理機構に対して上記ホストコンピュータについてのアクセス制限情報を通知するストレージエリア・ネットワーク管理システムにおいて、ホストコンピュータ、ホストコンピュータに設けられたホストバス・アダプタ、スイッチ、あるいは、ストレージ装置に設けられたファイバチャネル・アダプタが交換されたとき、上記統合管理機構はこれを検知し、上記ホストコンピュータのストレージエリア・ネットワーク管理機構、スイッチの領域設定機構、もしくは、ストレージ装置のストレージ管理機構から、交換後の設定情報を取得し、交換前と同等のアクセス関係を構築するように再度アクセス関係を設定することを特徴とするストレージエリア・ネットワーク・システム。

(付記5) ホストコンピュータのホストバス・アダプタが故障して交換された際、統合管理機構はホストバス・アダプタの交換を検知して、システム管理者に通知し、

システム管理者からの構成再設定コマンドにより、統合管理機構1は、ホストコンピュータのストレージエリア・ネットワーク管理機構に交換された新しいホストバス・アダプタの設定情報を伝え、該新しい設定情報を用いてホストバス・アダプタ交換前と同等のアクセス関係を構築し、ストレージエリア・ネットワーク管理機構、領域設定機構、ストレージ管理機構に再度アクセス関係を設定することを特徴とする付記4記載のストレージエリア・ネットワーク・システム。

(付記6) ホストコンピュータが故障して交換された際、統合管理機構は、ホストコンピュータのストレージエリア・ネットワーク管理機構の設定がなくなっている事を検知して、システム管理者に通知し、システム管理者からの構成再設定コマンドにより、上記ストレージエリア・ネットワーク管理機構は統合管理機構に対して接続されているホストバス・アダプタの設定情報を伝え、統合管理機構はその情報を用いてホストコンピュータ交換前と同等のアクセス関係を構築し、領域設定機構、ストレージ管理機構に再度アクセス関係を設定することを特徴とする付記4記載のストレージエリア・ネットワーク・システム。

(付記7) スイッチが故障して交換された際、統合管理機構は、スイッチに設定した領域設定情報がなくなっている事を検出し、システム管理者に通知し、システム管理者からの構成再設定コマンドによって、新しいスイッチに故障前のアクセス関係をセットさせ、アクセス関係を再設定できるようにしたことを特徴とする付記4記載のストレージエリア・ネットワーク・システム。

(付記8) スイッチが故障して交換された際に、スイッチに設定した領域設定情報がなくなっている事を検出し、統合管理機構は、自動的に新しいスイッチに故障前のアクセス関係をセットさせ、アクセス関係を再設定できるようにしたことを特徴とする付記4記載のストレージエリア・ネットワーク・システム。

(付記9) ストレージ装置側のファイバチャネル・アダプタ交換され、ファイバチャネル・アダプタの設定情報が変更された場合、統合管理機構は、これを検出し、システム管理者に通知し、システム管理者からの構成再設定コマンドによって、ストレージ管理機構が新しい設定情報を統合管理機構に伝え、統合管理機構はその新しい設定情報を用いて交換前と同等のアクセス関係を構築し、ストレージエリア・ネットワーク管理機構、領域設定機構に再度アクセス関係を設定することを特徴とする付記4記載のストレージエリア・ネットワーク・システム。

(付記10) 複数のホストコンピュータと複数のストレージ装置が、スイッチを介して接続されたストレージエリア・ネットワーク・システムであって、上記ストレージエリア・ネットワークを統合制御する統合管理機構を備え、該統合管理機構はホストコンピュータとストレ

タのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知し、スイッチの領域設定機構に対して領域情報を通知し、ストレージ装置のストレージ管理機構に対して上記ホストコンピュータについてのアクセス制限情報を通知することを特徴とするストレージエリア・ネットワーク・システムにおける統合管理機構。

(付記 19) 複数のホストコンピュータと複数のストレージ装置が、スイッチを介してファイバチャネルで接続されたストレージエリア・ネットワーク・システムを統合制御する統合管理プログラムであって、上記統合管理プログラムは、ホストコンピュータとストレージ装置とのアクセス経路情報に基づき、ホストコンピュータのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知する処理と、スイッチの領域設定機構に対して領域情報を通知する処理と、ストレージ装置のストレージ管理機構に対して上記ホストコンピュータについてのアクセス制限情報を通知する処理とをコンピュータに実行させ、ホストとストレージとのアクセス関係を一括して管理することを特徴とするストレージエリア・ネットワーク・システムを統合制御するプログラム。

(付記 20) 複数のホストコンピュータと複数のストレージ装置が、スイッチを介してファイバチャネルで接続されたストレージエリア・ネットワーク・システムを統合制御する統合管理プログラムを記録した記録媒体であって、上記統合管理プログラムは、ホストコンピュータとストレージ装置とのアクセス経路情報に基づき、ホストコンピュータのストレージエリア・ネットワーク管理機構に対して、ストレージ装置に対する管理情報を通知し、スイッチの領域設定機構に対して領域情報を通知し、ストレージ装置のストレージ管理機構に対して上記ホストコンピュータについてのアクセス制限情報を通知し、ホストとストレージとのアクセス関係を一括して管理することを特徴とするストレージエリア・ネットワーク・システムを統合制御するプログラムを記録した記録媒体。

【0038】

【発明の効果】以上説明したように、本発明においては、SANにストレージエリア・ネットワークを統合制御する統合管理機構を設け、ホストとストレージとのアクセス関係を上記統合管理機構により一括して管理するようにしたので、以下の効果を得ることができる。

(1) 信頼性の高い一元管理されたSANシステムを構築することができる。また、前記したホスト・アフィニティ、ゾーニング等の機能を持っていない、過去のシステムに対しても対応できるので、全て新しいシステムを購入してSANを構築することが動作環境の必須条件としない。

(2) SANの異常や、アクセスパスの整合性を容易に確認することができる。

(3) SANを構成するホスト、HAB、スイッチ、ストレージ装置、FCA等が交換され、SANの構成状態が変更されても容易に対応することができる。

(4) SANに異常が発生した場合、被疑箇所やその影響範囲を容易に特定することができ、業務影響を最小限に止めることができる。

【図面の簡単な説明】

【図 1】本発明の概要を説明する図である。

【図 2】本発明の対象となるSANシステムの構成例を示す図である。

【図 3】本発明の実施例のSAN管理システムの構成を示す図である。

【図 4】ストレージ装置のハードウェア構成例を示す図である。

【図 5】アクセスパス設定情報、ストレージ・アフィニティ・テーブル、スイッチ・ゾーニングテーブル、ホスト・アフィニティ・テーブルの例を示す図である。

【図 6】SAN統合管理機構が行う処理のフローチャートを示す図である。

【図 7】ゾーニング設定機構が行う処理のフローチャートを示す図である。

【図 8】SANの障害管理を説明する図である。

【図 9】障害報告方法定義の一例を示す図である。

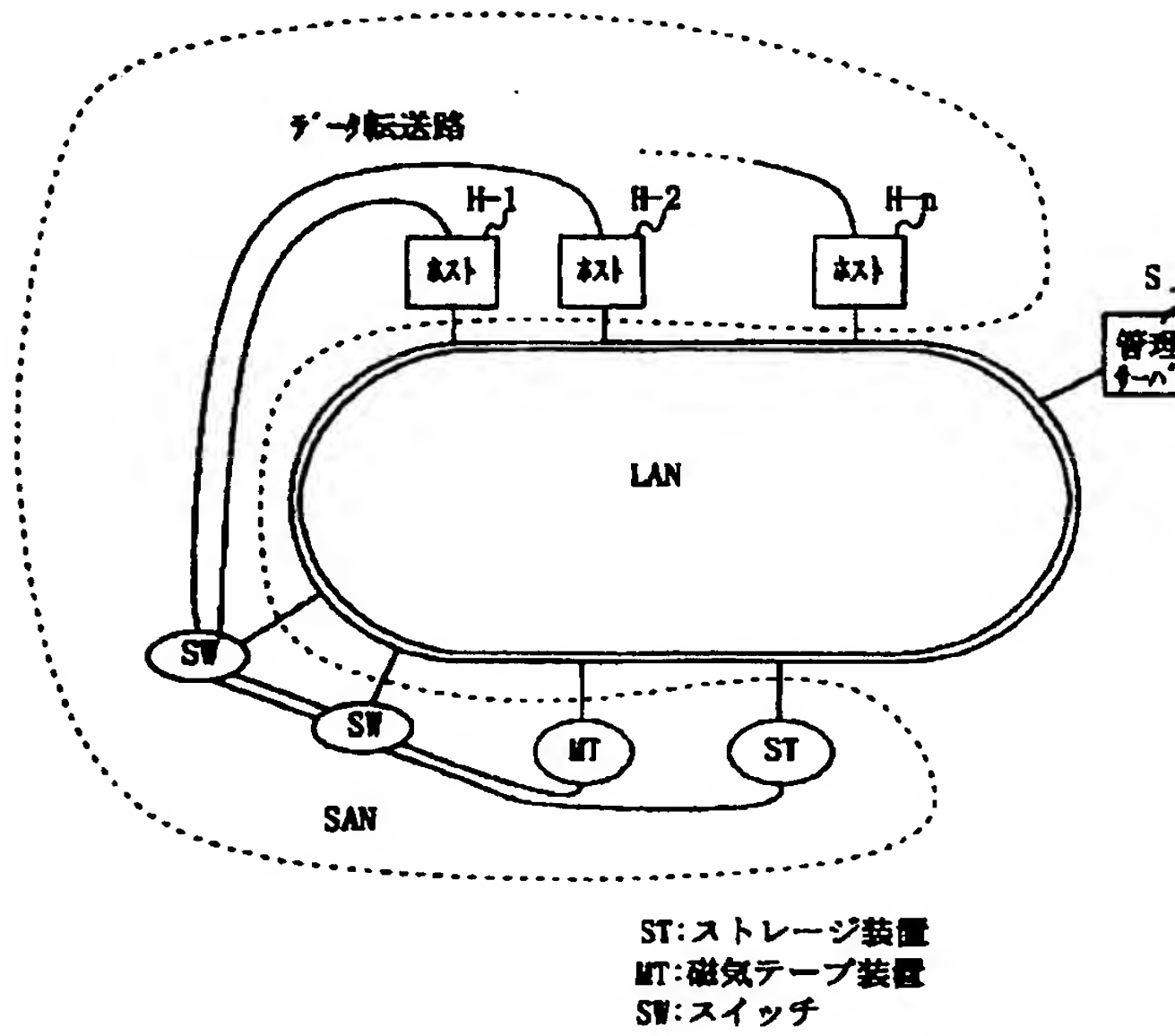
【図 10】SAN統合管理機構が行うSANの障害監視機能のフローチャートである。

【符号の説明】

1	統合管理機構
1 a	構成設定情報
2	ホスト
2 a	SAN管理機構
3	スイッチ
3 a	ゾーニング(Zoning)設定機構
4	ストレージ装置
4 a	ストレージ管理機構
1 1 0, 1 2 0	ホスト
1 1 1, 1 1 2	ホストバス・アダプタ (HBA)
1 2 1	ホストバス・アダプタ (HBA)
3 0 0	スイッチ
3 0 1	ゾーニング設定情報
4 1 0, 4 2 0	ストレージ装置
4 1 1, 4 2 1	ファイバチャネル・アダプタ (FCA)
4 2 1	ファイバチャネル・アダプタ (FCA)
4 1 8, 4 2 8	ストレージ管理機構
5 0 0	SAN統合管理機構
5 0 1	SAN構成設定情報

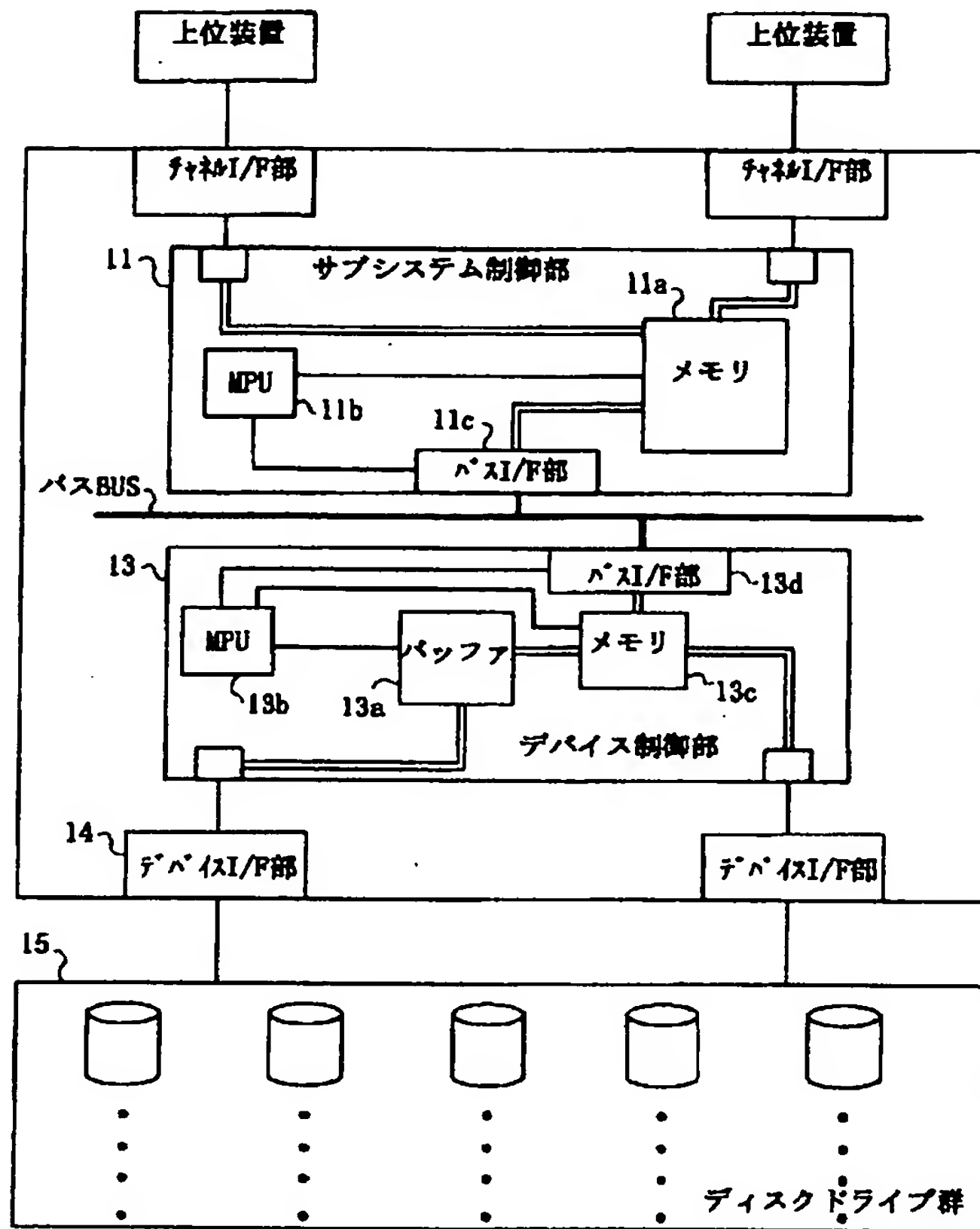
【図2】

本発明の対象となるSANシステムの構成例を示す図



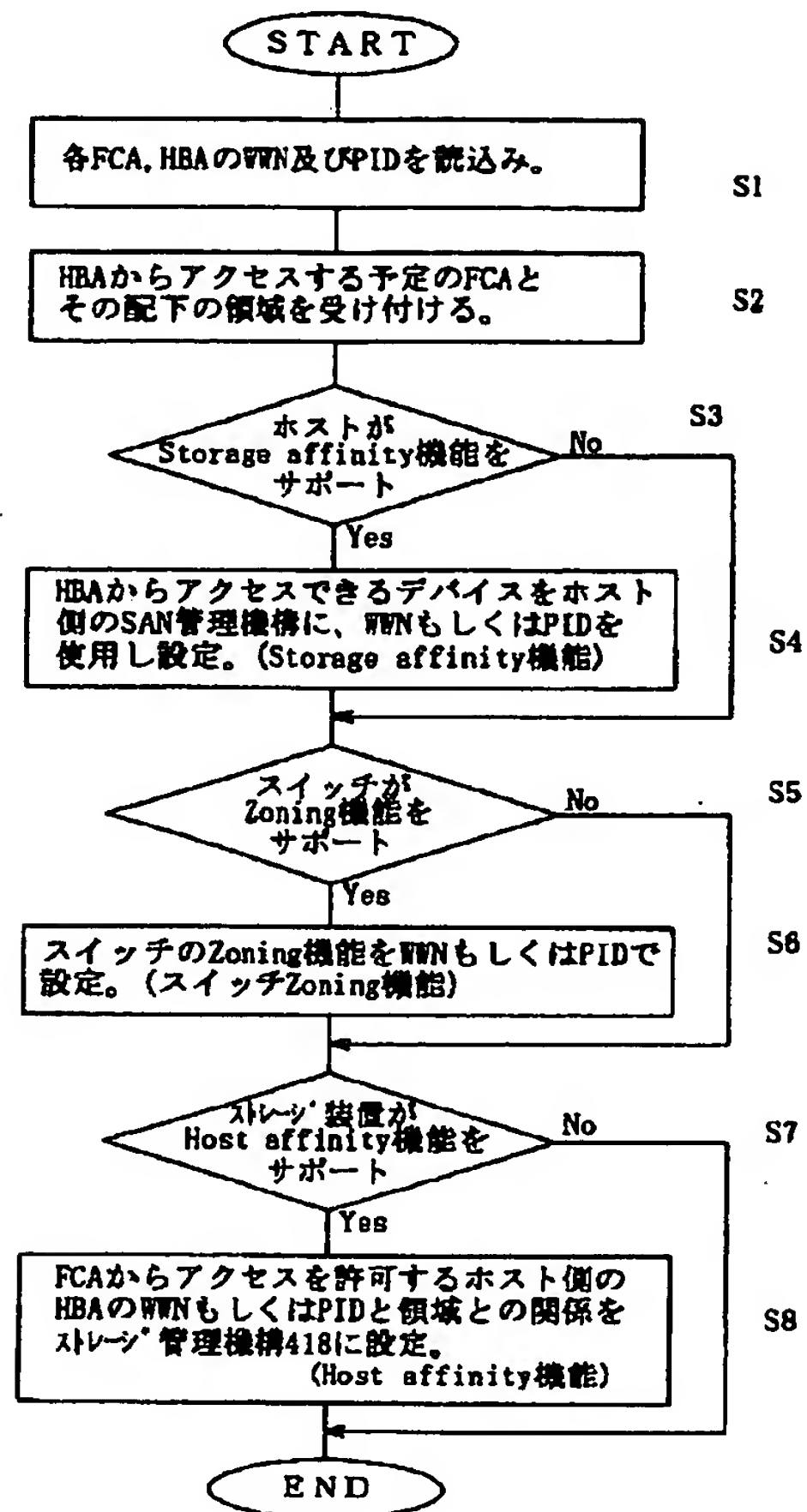
【図4】

本発明の実施例のストレージ装置のハードウェア構成例を示す図



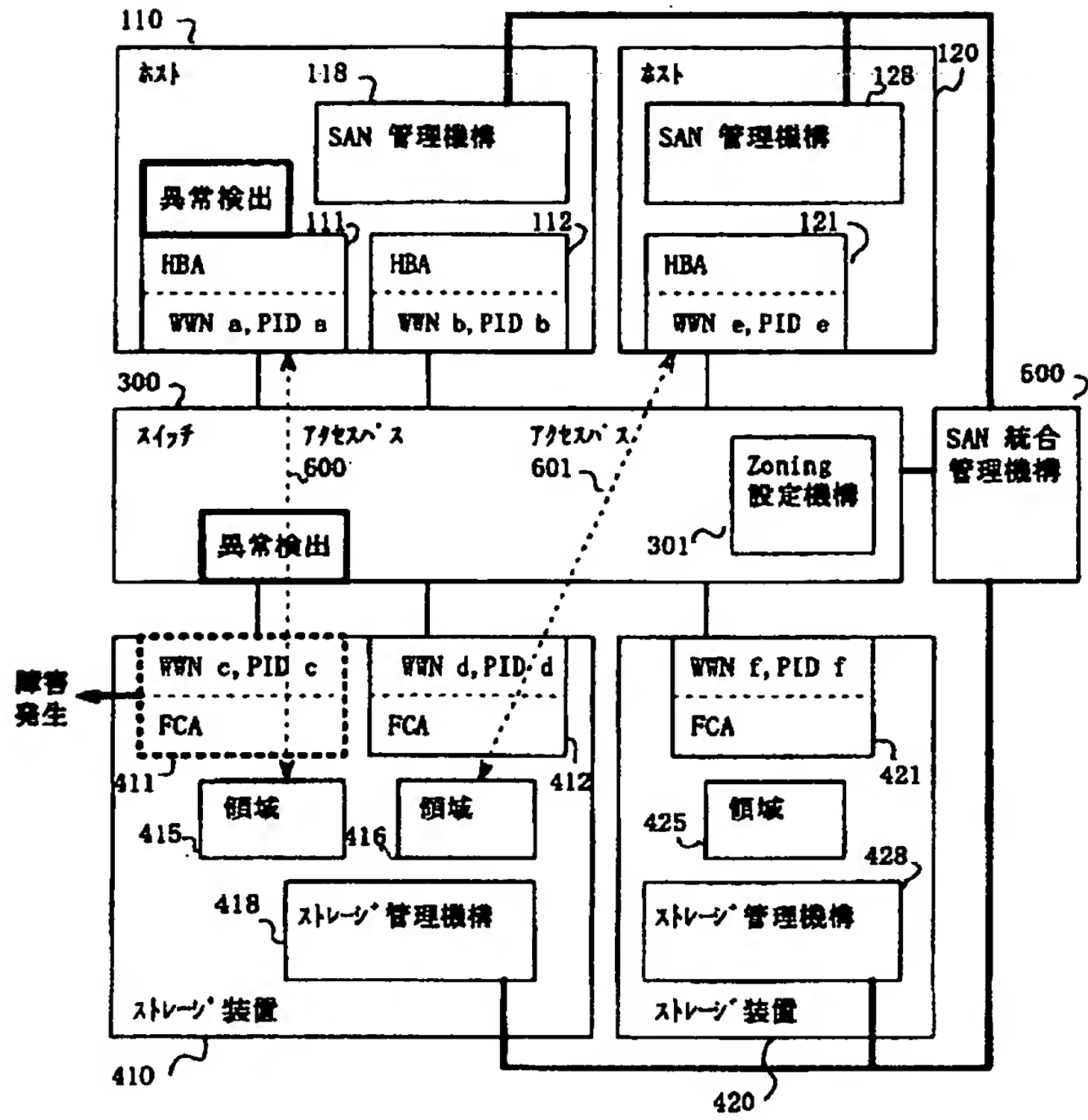
【図6】

SAN統合管理機構が行う処理のフローチャートを示す図



【図 8】

SANの障害管理を説明する図



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☒ **BLACK BORDERS**

☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**

☒ **FADED TEXT OR DRAWING**

☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**

☐ **SKEWED/SLANTED IMAGES**

☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**

☐ **GRAY SCALE DOCUMENTS**

☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**

☒ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**

☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.